ЛАБОРАТОРНАЯ РАБОТА №2
Управление системными службами и процессами Windows

1. Цель работы

Целью работы является освоение способов управления службами в ОС Windows 10, изучение специфики работы планировщика задач, а также ознакомление со структурой и особенностями работы процессов и потоков в операционных системах.

2. Краткие теоретические сведения

Служба Windows – программа или процесс, который выполняется в фоновом режиме, т.е. без прямого общения с пользователем, и обеспечивает поддержку других программ. Службы могут запускаться при загрузке операционной системы и находиться в оперативной памяти вплоть до завершения работы. Каждая служба имеет определённые характеристики: тип запуска, условия восстановления и другие, которые будут рассмотрены ниже.

Параметры настройки служб хранятся в реестре Windows.

Процесс services.exe, запущенный от имени пользователя SYSTEM, отвечает за запуск, остановку и управление службами. Services.exe автоматически запускает службы во время загрузки ОС и останавливает все службы при завершении работы Windows. Другое название этого процесса – диспетчер управления службами (Service control manager, SCM).

Отдельные службы запускаются в процессе svchost.exe, который является дочерним для services.exe. На компьютере может быть запущено несколько экземпляров процесса svchost.exe, при этом каждый из них содержит различные службы. Один экземпляр процесса svchost.exe может содержать одну службу для программы, а другой – несколько служб, относящихся к работе Windows.

Не только система, но и сам пользователь может управлять службами. В Windows предусмотрено управление службами через графический интерфейс и через командную строку, а также при помощи изменения ключей реестра.

3. Ход работы

3.1. Управление службами

Запустите диспетчер задач, нажав Ctrl+Alt+Del. Перейдите на вкладку «Службы» (рис. 1), чтобы увидеть все службы, установленные в операционной системе.

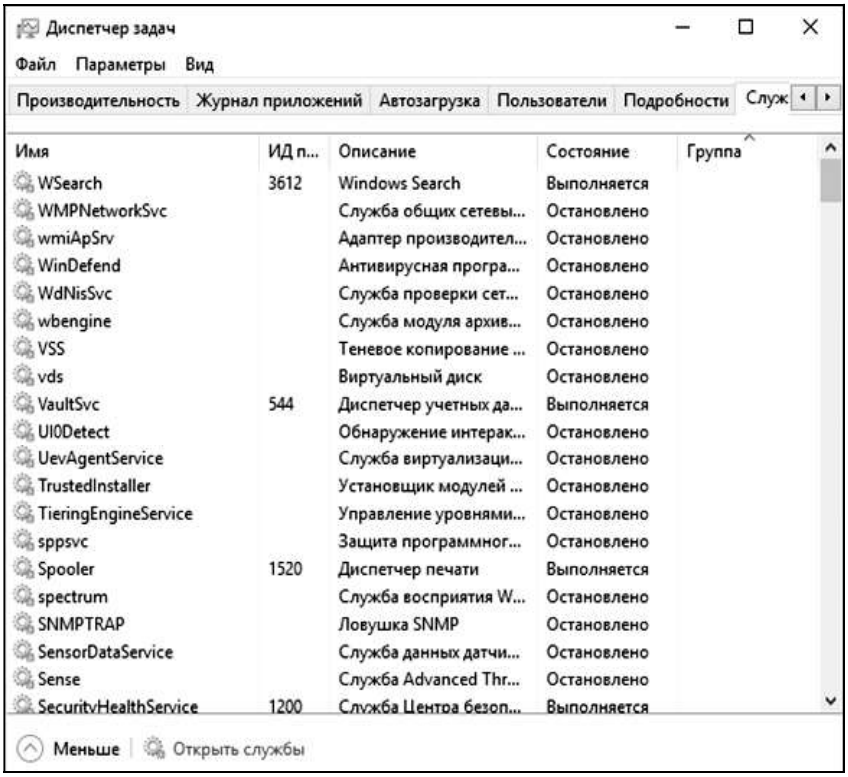

Рис. 1. Просмотр установленных служб в диспетчере задач

Для каждой службы в диспетчере задач показывается её имя, идентификатор процесса, в рамках которого она запущена (если такой имеется), краткое описание, текущее состояние и группа.

Диспетчер задач позволяет запускать и останавливать службы, если это возможно. Щёлкните правой кнопкой на службе из списка, чтобы увидеть возможные действия (рис. 2).

Запустите и остановите службу Parental Controls (WPCSvc). Приложения, выполняющие функции, аналогичные диспетчеру задач, также зачастую позволяют просматривать, запускать и останавливать службы. Например, эти возможности доступны в Process Explorer.

Оснастка !Службы! – другое средство управления службами, имеющее графический интерфейс, но обладающее большими возможностями, чем диспетчер задач. Оснастка «Службы» представляет собой оснастку консоли MMC.

Оснастку «Службы» можно запустить из диспетчера задач (начиная с Windows 7). Для этого нужно нажать кнопку «Открыть службы» на вкладке «Службы» (рис. 3).

Чтобы запустить оснастку «Службы» из командной строки, нужно выполнить services.msc. Окно оснастки представлено на рис. 4.

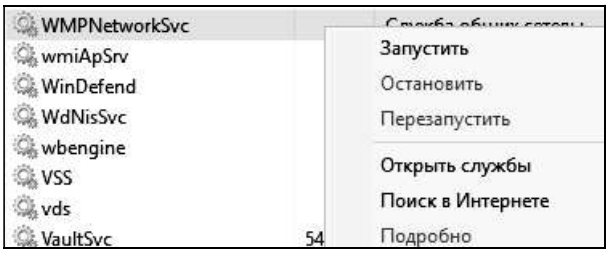

Рис. 2. Действия со службами в диспетчере задач

Рис. 3. Вызов оснастки из диспетчера задач

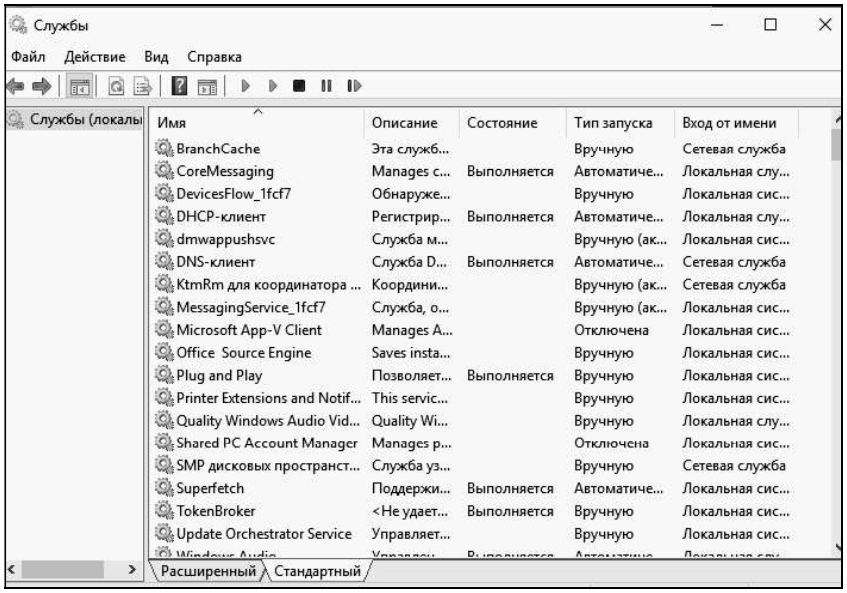

Рис. 4. Оснастка «Службы»

Если два раза щёлкнуть левой кнопкой мыши по любой из доступных служб, откроется окно свойств этой службы (рис. 5).

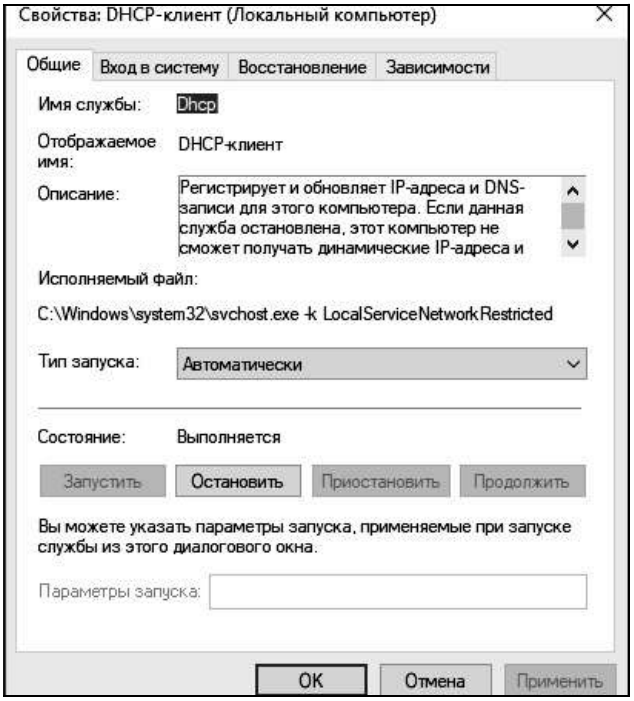

Рис. 5. Окно свойств службы

Служба может находиться в одном из следующих состояний: работает, приостановлена и остановлена. Соответственно, для службы доступно 4 команды: запустить, остановить, приостановить, продолжить. Эти команды для выбранной службы отображаются в оснастке слева от списка доступных служб (при выборе «расширенного» вида внизу окна), либо в окне свойств выбранной службы на вкладке «Общие». Команды также отображаются, если щёлкнуть правой кнопкой на службе в списке.

Не все службы могут быть приостановлены – некоторые могут быть только запущены и остановлены. Некоторые службы нельзя ни приостановить, ни остановить.

Остановите службу «Windows Audio» и попробуйте запустить звуковой файл. Затем запустите службу и убедитесь, что файл проигрывается.

Служба может зависеть от других служб и при этом могут быть службы, зависящие от неё. Если служба, от которой зависит данная

служба, не запущена, то данная служба может работать некорректно или вообще не запуститься.

Одна служба может иметь несколько зависимых служб. Также сама служба может быть зависима от нескольких служб. Службы могут зависеть не только от других служб, но и от некоторых драйверов. Зависимые службы можно просмотреть на вкладке «Зависимости» окна свойств службы (рис. 6).

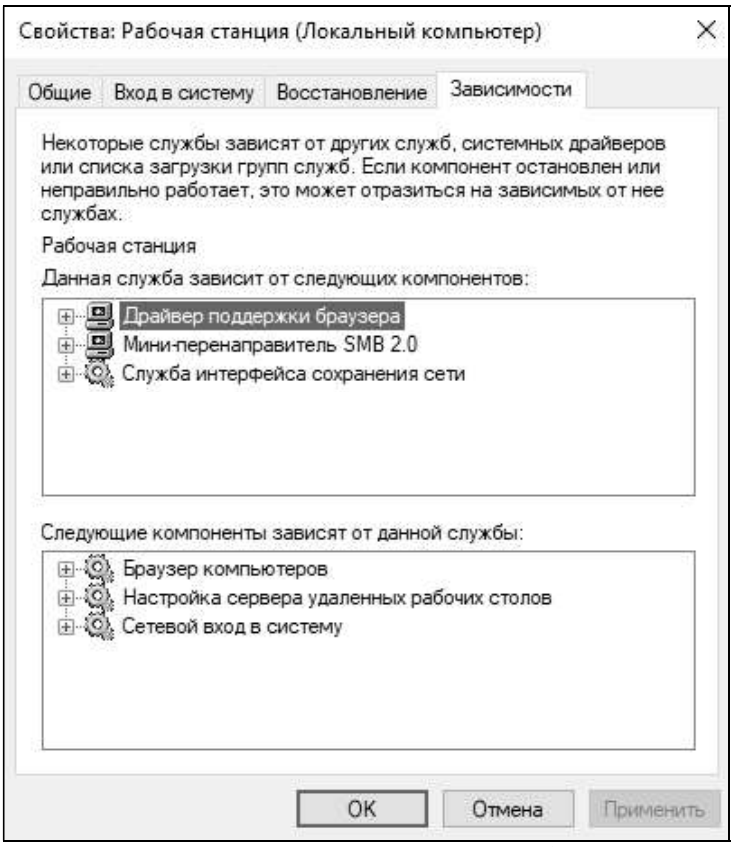

Рис. 6. Просмотр зависимостей службы

Остановите службу «Система событий COM+», которая имеет зависимую службу «Служба уведомления о системных событиях». Система выведет предупреждение о том, что зависимые службы будут также остановлены (рис. 7).

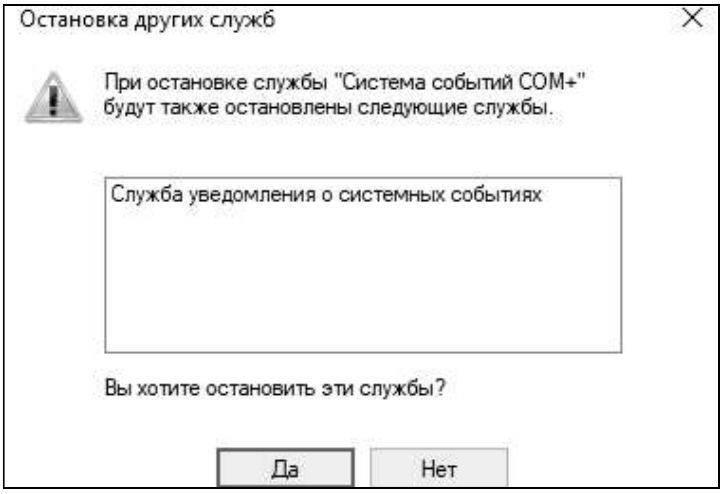

Рис. 7. Попытка остановить службу с зависимостями

Каждая служба может иметь один из следующих типов запуска:

– автоматически: служба запускается при загрузке Windows;

– вручную: служба запускается пользователем в оснастке «Службы» или любым другим способом;

– отключена: служба не может быть запущена, пока тип запуска не будет сменён на другой.

Кроме того, имеются также два дополнительных типа запуска: первый – запуск на этапе загрузке ядра Windows (низкоуровневые драйверы), второй – запуск сразу после инициализации ядра. Для таких служб сменить тип запуска в оснастке нельзя (например, служба «Удалённый вызов процедур»).

Примечание: начиная с Windows Vista, у служб присутствует ещё один тип запуска – «Автоматически (отложено)». Он аналогичен типу «Автоматически», но запускает службу через некоторое время после загрузки для оптимизации запуска Windows.

Тип запуска можно сменить на вкладке «Общие» окна свойств службы. Для службы «Темы» установите тип запуска «Вручную», перезагрузите компьютер и убедитесь, что окна Windows имеют «классический» вид, так как служба не запущена.

Если работа службы была некорректно завершена, Windows может перезапустить её или выполнить другие действия. Настройка параметров восстановления находится на вкладке «Восстановление» окна свойств службы (рис. 8).

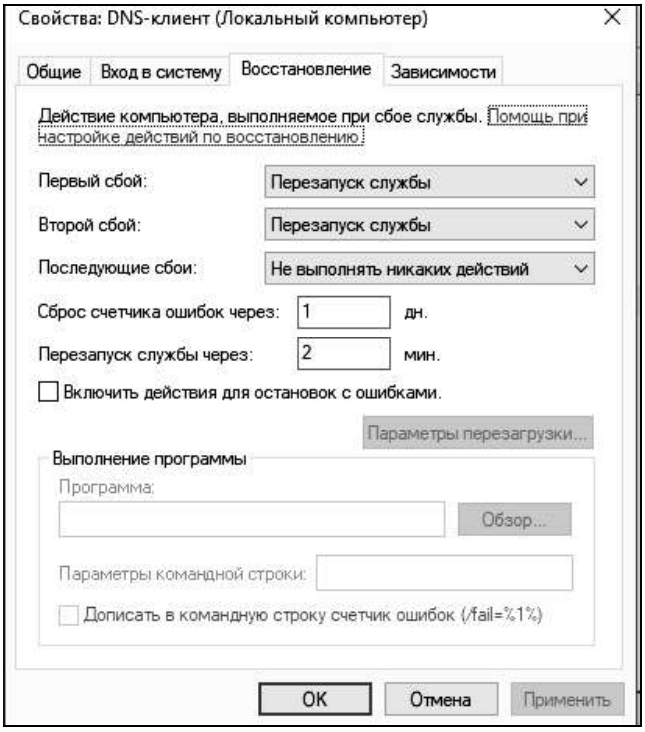

Рис. 8. Параметры восстановления службы

Можно задать действия, которые будут выполняться при первом, втором и последующих сбоях службы. Среди доступных действий:

– перезапуск службы: перезапускает службу через указанное время после сбоя;

– запуск программы: запускает выбранную ниже программу с заданными параметрами командной строки. Можно включить в параметры командной строки номер очередного сбоя службы;

– перезагрузка компьютера: перезагружает компьютер немедленно или по истечении заданного времени. При этом можно вывести на экран сообщение о неминуемой перезагрузке;

– не выполнять никаких действий: никакие действия после сбоя выполнены не будут.

Некоторые службы, например «Plug'n'play», не поддерживают параметры восстановления. Обычно при сбое этих служб компьютер перезагружается.

Установите параметры восстановления для службы «Диспетчер печати» («Диспетчер очереди печати») следующим образом: при первом сбое служба должна мгновенно перезапускаться, при втором – перезагружать компьютер с выводом сообщения через 2 минуты.

Завершите процесс spoolsv.exe, в котором запущена эта служба. Убедитесь, что процесс тут же запускается снова. Завершите процесс второй раз и убедитесь, что Windows выводит сообщение о неминуемой перезагрузке и через 2 минуты компьютер перезагружается.

Каждая служба имеет определённые права при запуске. Служба может запускаться:

– с системной учётной записью;

– как локальная служба;

– как сетевая служба;

– с правами какого-либо пользователя.

Права службы можно сменить на вкладке «Вход в систему» окна свойств службы (рис. 9).

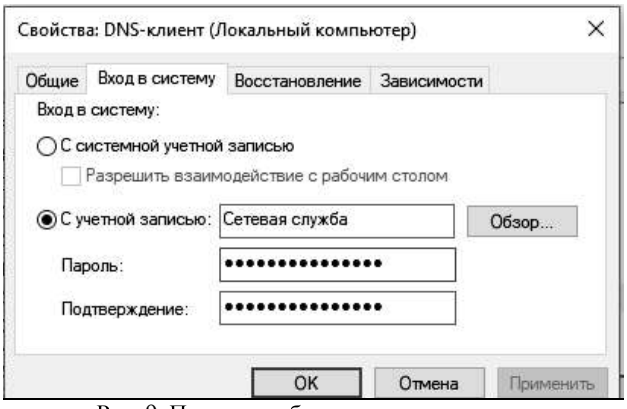

Рис. 9. Права службы при входе в систему

Чтобы выбрать вход с системной учётной записью, выберите соответствующий вариант вверху окна. Для выбора локальной службы нужно ввести в качестве имени пользователя «NT AUTHORITY / LocalService» («Локальная служба» в Windows Vista и 7) без кавычек, а пароль не вводить.

Для выбора сетевой службы – «NT AUTHORITY/NetworkService» («Сетевая служба» в Windows Vista и 7) и пароль так же не вводить.

Для работы со службами из командной строки предусмотрены команды семейств net и sc. Семейство net в основном используется для

других целей и имеет базовые команды работы со службами. Семейство sc, введённое в Windows XP, целиком посвящено работе со службами.

Запустите командную строку, выбрав «Пуск > Выполнить» и набрав cmd.

Для просмотра запущенных на данный момент служб введите команду net start. Обратите внимание, что она выводит список отображаемых имён служб, а не сами имена служб (рис. 10).

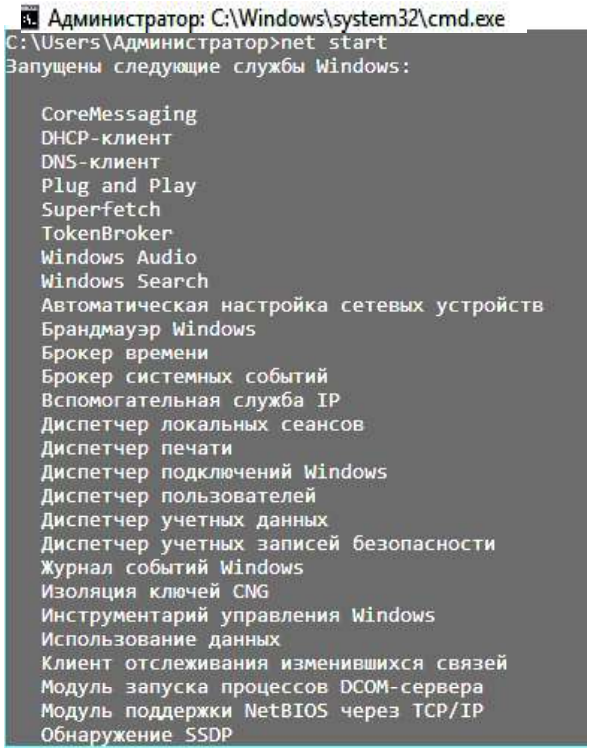

Рис. 10. Выполнение команды net start

Чтобы запустить службу, введите команду net start с последующим именем службы. Запустите службу SysmonLog (pla начиная с Windows 7) – «Журналы и оповещения производительности» (рис. 11).

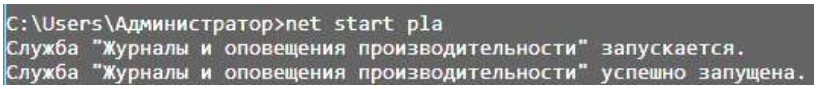

Рис. 11. Запуск службы с помощью net start

Если служба имеет тип запуска «Отключена» или уже запущена, об этом будет выведено соответствующее сообщение.

Для остановки службы используется команда net stop с последующим именем службы. Если служба не запущена или не может быть остановлена, об этом будет выведено сообщение. Остановите службу MpsSvc – «Брандмауэр Windows». Зайдите в панель управления и убедитесь, что брандмауэр Windows отключен.

Команды семейства net не позволяют, например, выводить все установленные в системе службы. Для этого используются команды семейства sc.

Семейство sc позволяет просматривать и изменять подробную информацию о каждой службе, а также регистрировать в системе новые службы и удалять установленные. Если ввести sc без параметров, можно просмотреть справку по этому семейству. То же самое относится к большинству команд этого семейства.

Для вывода списка служб используются команды sc query и sc queryex. Первая команда выводит такие данные о службе, как имя (SERVICE_NAME), отображаемое имя (DISPLAY_NAME), состояние (STATE) и другие данные, не рассматриваемые в данной работе. Вторая команда дополнительно выводит идентификатор процесса (PID), в рамках которого запущена служба (рис. 12).

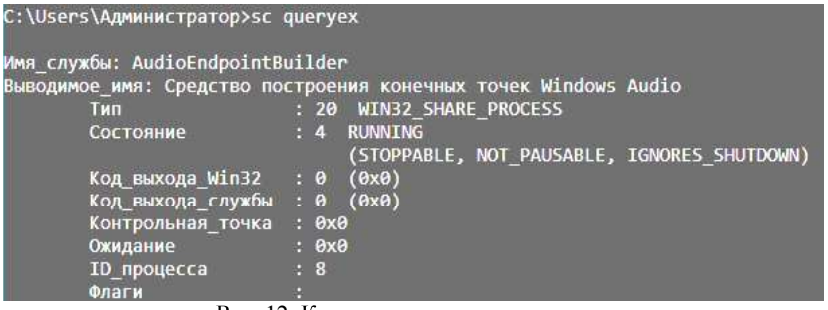

Рис. 12. Команды sc query и sc queryex

Команды позволяют использовать фильтр для вывода списка служб. Фильтр задаётся в виде параметров, введённых после команды. Среди параметров:

– type: имеет значение driver (драйвер), service (служба), interact (интерактивная служба, которая обменивается информацией с пользователем) или all (и то, и другое). По умолчанию – service;

– state: имеет значение inactive (незапущенные службы) или all (и запущенные, и остановленные службы). Если параметр не задан, он принимается равным значению active (запущенные службы).

Таким образом, чтобы, например, вывести список незапущенных служб драйверов, нужно ввести команду sc query type= all state= inactive.

Соответственно, если не задано никаких параметров, выводятся все запущенные службы.

Если после команды sc query или sc queryex ввести имя службы, будет выведена информация только об этой службе.

Выведите список всех установленных интерактивных служб. Затем выведите расширенную информацию об одной из запущенных служб из этого списка.

Кроме перечисленных команд, для вывода информации о конкретной службе используются также команды sc qc, sc qdescription, sc qfailure и другие. После команды пишется имя соответствующей службы (рис. 13).

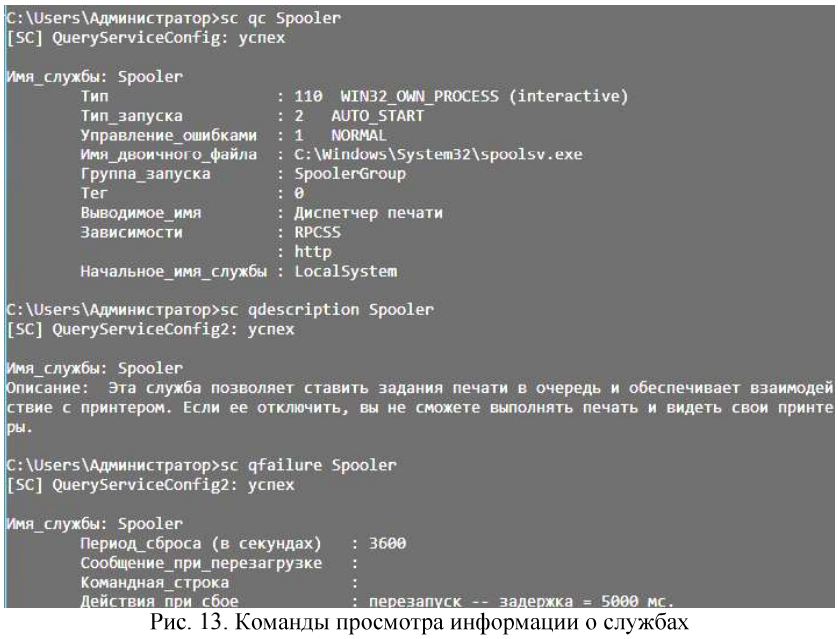

Рис. 13. Команды просмотра информации о службах

sc qc выводит такую информацию: тип запуска службы (START_TYPE), имя исполняемого файла (BINARY_PATH_NAME), отображаемое имя (DISPLAY_NAME), зависимости (DEPENDENCIES) и имя учётной записи, правами которой обладает служба при запуске (или начальное имя службы, SERVICE_START_NAME).

sc qdescription выводит описание службы (DESCRIPTION).

sc qfailure выводит действия при сбое службы (FAILURE_ ACTIONS), период сброса счётчика сбоев в секундах (RESET_PERIOD), сообщение при неминуемой перезагрузке (REBOOT_MESSAGE) и путь к файлу программы для запуска (COMMAND_LINE).

Кроме того, можно вывести список служб, зависящих от данной службы. Для этого используется команда sc enumdepend.

Выведите информацию с помощью этих команд о службе CryptSvc – «Службы криптографии».

Для изменения состояния службы используются следующие команды:

– sc start: запуск службы;

– sc pause: приостановка службы, если возможно;

– sc continue: продолжение работы службы, если она была приостановлена;

– sc stop: остановка службы, если возможно.

После команды пишется имя службы, состояние которой нужно изменить.

Для изменения типа запуска определённой службы используется команда sc config с последующим именем службы и списком изменяемых параметров. Эта команда также позволяет, в частности, изменять имя учётной записи для службы, отображаемое имя, путь к исполняемому файлу и даже зависимости, что недоступно в диспетчере управления службами.

Для изменения типа запуска используется параметр start. Его значения:

– boot: запуск при инициализации ядра Windows;

– system: запуск сразу после инициализации ядра Windows;

– auto: запуск сразу после загрузки Windows (соответствует типу «Автоматически» в диспетчере управления службами);

– demand: запуск по требованию пользователя (соответствует типу «Вручную» в диспетчере управления службами);

– disabled: служба отключена (соответствует типу «Отключена» в диспетчере управления службами).

Примечание: для Windows Vista и выше, типу «Автоматически (отложено)» соответствует значение параметра delayed-auto.

Примечание: как и в оснастке «Службы», первые два типа запуска изменять не допускается.

Таким образом, чтобы, например, установить службе «DNS-клиент» тип запуска «Вручную», нужно ввести sc config Dnscache start= demand.

С помощью этой команды измените тип запуска службы Themes – «Темы» на «Автоматически». Перезагрузите компьютер и убедитесь, что окна Windows имеют обычный вид.

Для изменения параметров восстановления определённой службы используется команда sc failure с последующим именем службы и списком изменяемых параметров. Параметры следующие:

– actions: действия, выполняемые при сбое и задержки перед их выполнением в миллисекундах. Сначала пишется действие при первом сбое, затем задержка, отделяемая от него косой чертой («/»). Если нужно задать действия при следующих сбоях, далее снова ставится косая черта и пишется следующее действие и задержка. Возможные действия:

– run: запуск программы. При использовании этого значения должен быть задан параметр command;

– reboot: перезагрузка компьютера. Используется совместно с параметром reboot;

– restart: перезапуск службы.

Чтобы при сбое не выполнялось никаких действий, просто не вводите следующее действие и его задержку.

К примеру, если службу при первом и втором сбое нужно перезапустить через 2 секунды, а при следующих сбоях – перезагрузить компьютер через 30 секунд, значение параметра actions будет равно restart/2000/restart/2000/reboot/30000;

– reset: продолжительность периода (в секундах), после которого счётчик сбоев сбрасывается. Если значение равно INFINITE, счётчик никогда не сбрасывается;

– reboot: сообщение, выводимое перед перезагрузкой;

– command: путь и параметры командной строки для файла запускаемой при сбое программы.

Для службы Spooler установите следующие параметры восстановления: при первом сбое служба должна перезапуститься через 5 секунд, при втором

– через 10 секунд, при третьем – компьютер должен перезагрузиться через 20 секунд с выводом соответствующего сообщения. Счётчик сбоев должен быть сброшен через 1 час.

Завершите процесс spoolsv.exe три раза, чтобы убедиться в правильности введённой команды.

Команда sc interrogate используется совместно с открытой оснасткой «Службы». При изменении состояния службы с помощью командной строки оно не сразу обновляется в оснастке. Чтобы принудительно обновить его, вводится эта команда с последующим именем службы.

Откройте оснастку «Службы». Остановите с помощью sc stop службу TapiSrv – «Телефония», а затем обновите её состояние в оснастке с помощью sc interrogate и убедитесь в том, что в оснастке её состояние показывается правильно.

Для регистрации новой службы в реестре используется команда sc create. При этом после команды требуется указать имя создаваемой службы и путь к исполняемому файлу (параметр binPath). Дополнительно можно указать тип запуска (start), зависимости (depend), отображаемое имя (DisplayName), имя (obj) и пароль (password) учётной записи для входа и другое.

Создайте новую службу, выбрав в качестве исполняемого файла Notepad.exe (блокнот) (рис. 14). Задайте ему автоматический тип запуска и произвольное отображаемое имя. Пусть служба обладает правами пользователя «Система» (LocalSystem).

```
C:\Users\Администратор>sc create Notepad binPath=C:\Windows\notepad.exe start=
auto DisplayName= Блокнот obj= LocalSystem
[SC] CreateService: успех
```

Рис. 14. Создание новой службы

Откройте оснастку «Службы» и убедитесь, что созданная служба отображается в списке.

Примечание: не пытайтесь запустить созданную службу. Она не отвечает требованиям, предъявляемым к службам, и приведена только в качестве примера.

Чтобы удалить службу, используется команда sc delete с последующим именем службы. Если служба запущена или используется другим процессом, она будет помечена для удаления и удалена позже.

Удалите только что созданную службу. Перейдите в оснастку «Службы», выберите «Действие > Обновить» и убедитесь, что служба в списке отсутствует.

Приведём описание некоторых системных служб Windows:

– DHCP-клиент: управляет конфигурацией сети посредством регистрации и обновления IP-адресов и DNS-имен.

– DNS-клиент: разрешает для данного компьютера DNS-имена в адреса и помещает их в кэш. Если служба остановлена, не удастся разрешить DNS-имена и разместить службу каталогов Active Directory контроллеров домена.

– Plug'n'play: позволяет компьютеру распознавать изменения в установленном оборудовании и подстраиваться под них, либо не требуя вмешательства пользователя, либо сводя его к минимуму.

– Windows audio: управление звуковыми устройствами для Windows-программ.

– Автоматическое обновление: загрузка и установка обновлений Windows. Если служба отключена, то на этом компьютере нельзя будет использовать возможности автоматического обновления или веб-узел Windows Update.

– Веб-клиент: позволяет Windows-программам создавать, получать доступ и изменять файлы, хранящиеся в Интернете.

– Диспетчер логических дисков: обнаружение и наблюдение за новыми жесткими дисками и передача информации о томах жестких дисков службе управления диспетчера логических дисков.

– Журнал событий: обеспечивает поддержку сообщений журналов событий, выдаваемых Windows-программами и компонентами системы, и просмотр этих сообщений.

– Обозреватель компьютеров/браузер компьютеров: обслуживает список компьютеров в сети и выдает его программам по запросу.

– Планировщик заданий: позволяет настраивать расписание автоматического выполнения задач на компьютере.

– Поставщик поддержки безопасности NT LM: аутентификация на серверах NT и доступ к ресурсам домена.

– Рабочая станция: обеспечивает поддержку сетевых подключений и связь. Если служба остановлена, программа, данные подключения будут недоступны.

– Сервер: обеспечивает поддержку общий доступ к файлам, принтерам и именованным каналам для данного компьютера через сетевое подключение.

– Сетевые подключения: управляет объектами папки «Сеть и удаленный доступ к сети», отображающей свойства локальной сети и подключений удаленного доступа.

– Служба восстановления системы: выполняет функции восстановления системы.

– Службы криптографии: предоставляет три службы управления: службу баз данных каталога, которая проверяет цифровые подписи файлов Windows; службу защищенного корня, которая добавляет и удаляет сертификаты доверенного корня центра сертификации с этого компьютера; и службу ключей, которая позволяет подавать заявки на сертификаты с этого компьютера. Начиная с Windows Vista, предоставляет также четвёртую службу: службу автоматического обновления корневых сертификатов, которая получает корневые сертификаты из центра обновления Windows и разрешает сценарии, такие как SSL.

– Теневое копирование тома: управляет созданием теневых копий (контрольных точек состояния) дисковых томов, которые используются для архивации и восстановления или для иных целей.

– Удалённый вызов процедур: выполняет запросы активации объектов, разрешение экспортера объектов и распределенный сбор мусора для серверов COM и DCOM.

– Управление приложениями: обеспечивает службы установки программного обеспечения, такие как назначение, публикация и удаление.

– Центр обеспечения безопасности: ведет наблюдение за настройками и параметрами безопасности системы.

3.2. Автоматизация выполнения административных задач

Планировщик заданий – это оснастка MMC, позволяющая назначать автоматически выполняемые задания, запуск которых производится в определенное время или при возникновении определенных событий.

Планировщик заданий содержит библиотеку всех назначенных заданий, обеспечивая возможность быстрого просмотра и удобного управления заданиями. Из библиотеки можно запустить, отключить, изменить и удалить задание.

Для того чтобы запустить планировщик задач, необходимо проверить, включена ли данная служба, как показано на рис. 15.

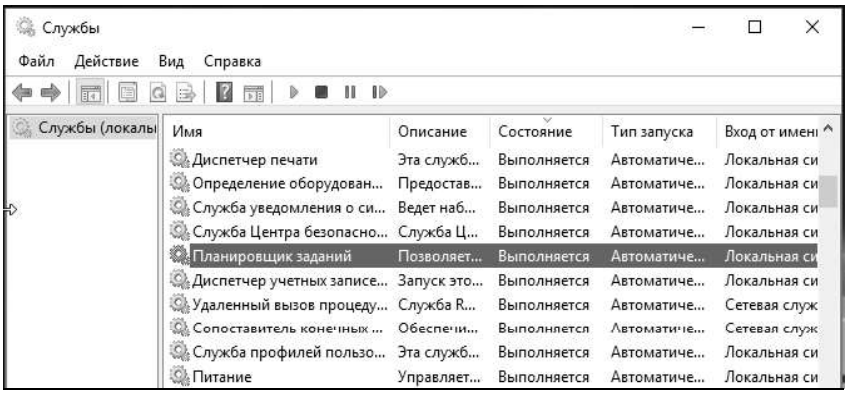

Рис. 15. Службы

Если служба Планировщик задач не включена, нужно вызвать контекстное меню, кликнув правой кнопкой мыши на данную службу и выбрать Свойства. Во вкладке Общее, если в поле Состояние стоит статус «Работает», значит служба планировщик задач запущена. Если нет, необходимо нажать кнопку «Запустить», тип запуска выбрать «Автоматически» и сохранить настройки (рис. 16).

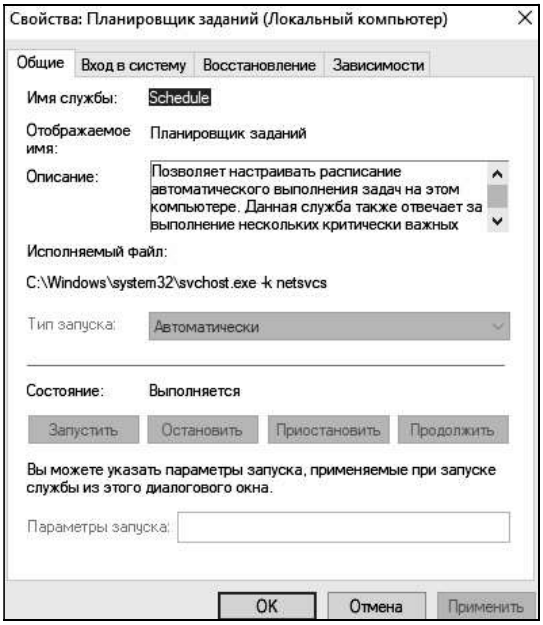

Рис. 16. Планировщик заданий

После того, как служба запущена и тип запуска автоматический, служба будет стартовать при загрузке системы, и задания будут выполняться в соответствии с выбранным расписанием.

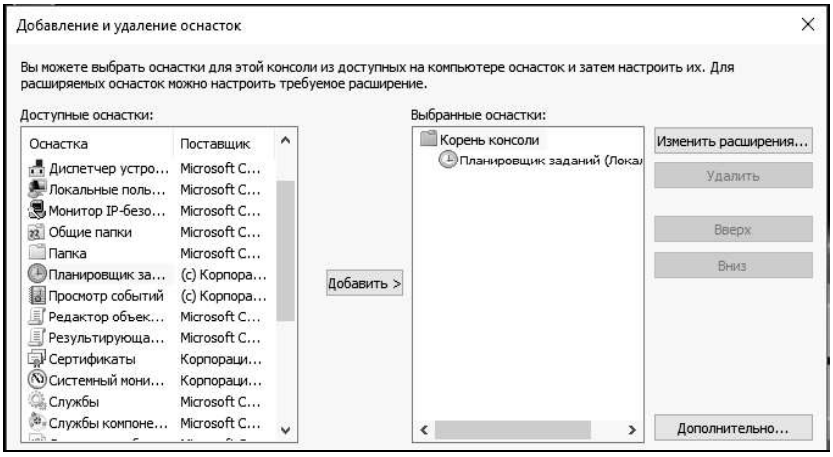

Рис. 17. Добавление оснастки

Чтобы создать задачу, потребуется сперва вызвать консоль управления MMC и добавить в нее оснастку «Планировщик заданий» (рис. 17). После чего в меню действий к данной оснастке выбрать пункт «Создать задачу…» или «Создать простую задачу…» (рис. 18).

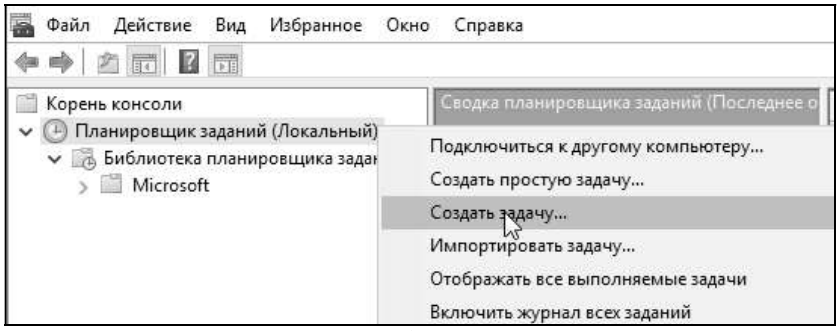

Рис. 18. Добавить задание

В случае выбора создания простой задачи – будет запущен «Мастер создания простой задачи», в котором по шагам будет предложено создать необходимое задание. Создайте задачу по запуску командной строки. Для удобства работы с создаваемыми задачами – каждой из них присваивается имя (рис. 19).

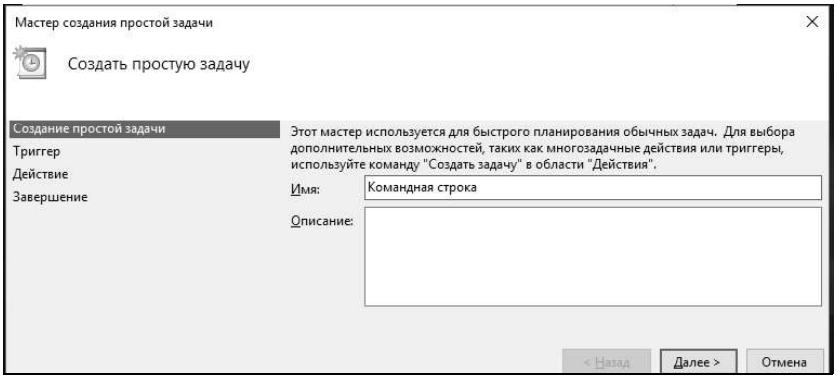

Рис. 19. Задание имени задаче

Мастер предложить указать период запуска этого задания. Возможны следующие варианты периода запуска задания:

– Ежедневно. Задание будет запускаться ежедневно, либо только по рабочим дням или через несколько дней в указанное время.

– Еженедельно. Указывается, каждую ли неделю нужно запускать задание и выбирать дни недели, по которым задание будет запущено в определенное время.

– Ежемесячно. В какие месяцы года надо запускать задание и выбирать по каким числам месяца, либо по каким дням месяца в определенное время будет запущено задание.

– Однократно. Можно выбрать дату и время запуска задания. Больше это задание выполняться не будет.

– При загрузке компьютера. При таком типе запуска задание будет выполняться каждый раз при загрузке компьютера. Данный тип запуска не требует входа пользователя.

– При входе в Windows. Этот тип запуска похож на предыдущий с тем отличием, что задание будет выполнено только когда пользователь войдет в Windows, то есть введет свои логин и пароль.

Выберите «При входе в Windows» и нажмите «Далее» (рис. 20).

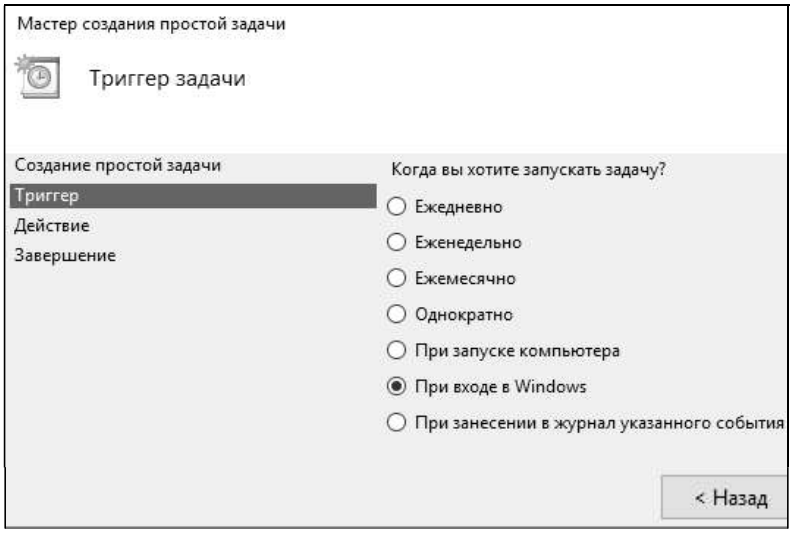

Рис. 20. Задание триггера запуска

Затем будет предложено выбрать действие, выполняемое задачей. Выберите «Запуск программы» (рис. 21). Будет предложено через «Проводник» указать файл программы, который будет необходимо запустить. Выберите из списка Командную строку (C:\Windows\System32\cmd.exe) и нажмите «Далее» (рис. 22).

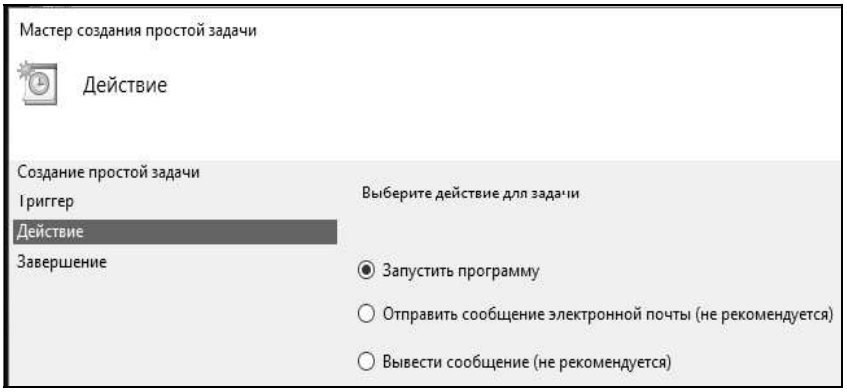

Рис. 21. Выбор действия

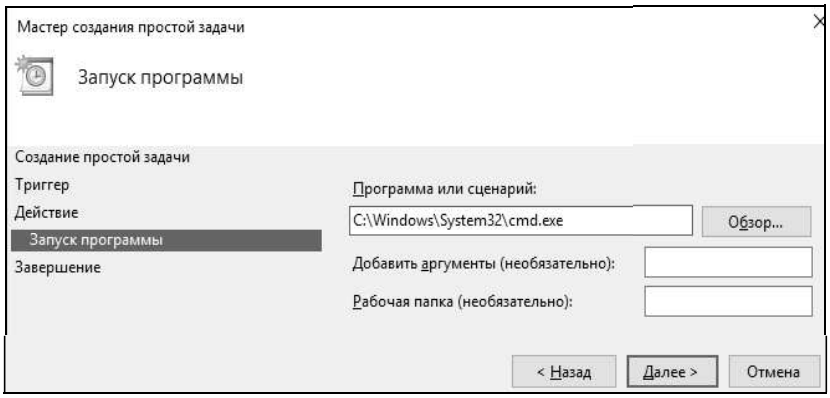

Рис. 22. Выбор программы для запуска

После проделанных действий «Мастер создания простой задачи» предоставит информацию по заданной задаче. Убедитесь, что все соответствует выбранным параметрам и нажмите «Готово» (рис. 23).

В библиотеке планировщика заданий появится новая задача с указанным Вами именем. Выделите задачу правой кнопкой и в меню действий (рис. 24) выберите пункт «Выполнить». Убедитесь, что задача осуществляется, после чего откройте ее свойства (рис. 25).

Ознакомьтесь с содержимым вкладок свойств созданной задачи. После чего запустите через меню действий планировщика «Создать задачу…». В данном формате создания задачи – мастер отличается от меню свойств созданной задачи только отсутствием вкладки «Журнал». Создайте через данный мастер задачу по запуску «Блокнота».

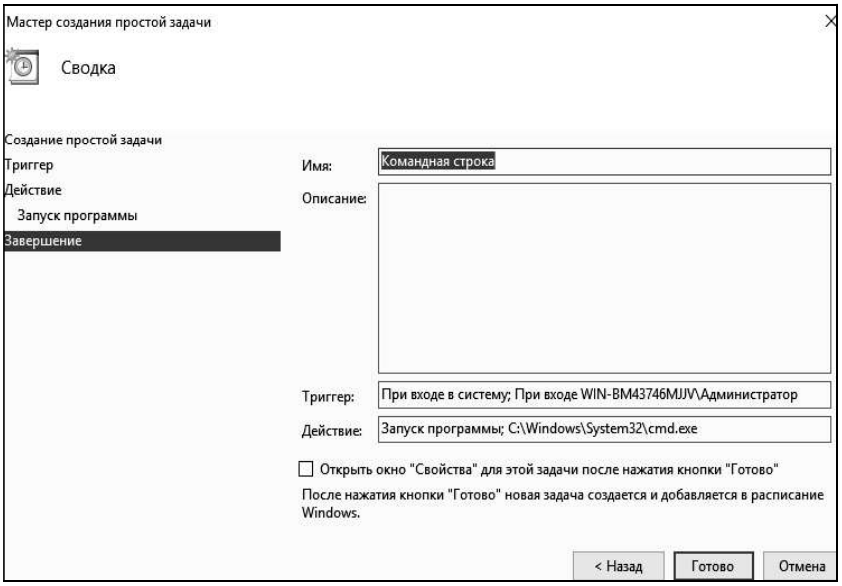

Рис. 23. Завершение работы мастера создания простой задачи

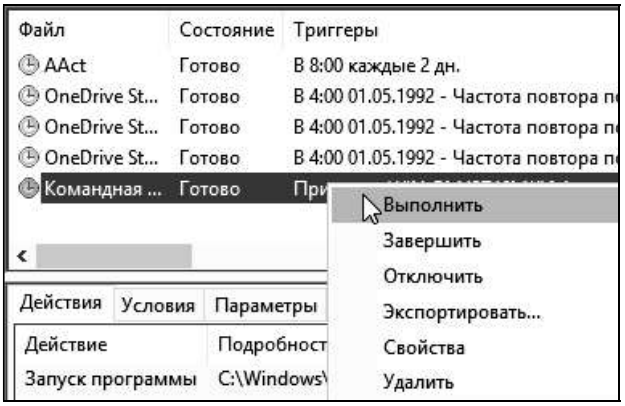

Рис. 24. Выбор действий с созданной задачей.

Добавьте в планировщик заданий Дефрагментацию диска. Для этого в Мастере планирования задания необходимо нажать Обзор и выбрать программу Defrag.exe, находящуюся в каталоге C:\Windows\System32\Defrag.exe (рис. 27). Выберите ежедневное выполнение задания.

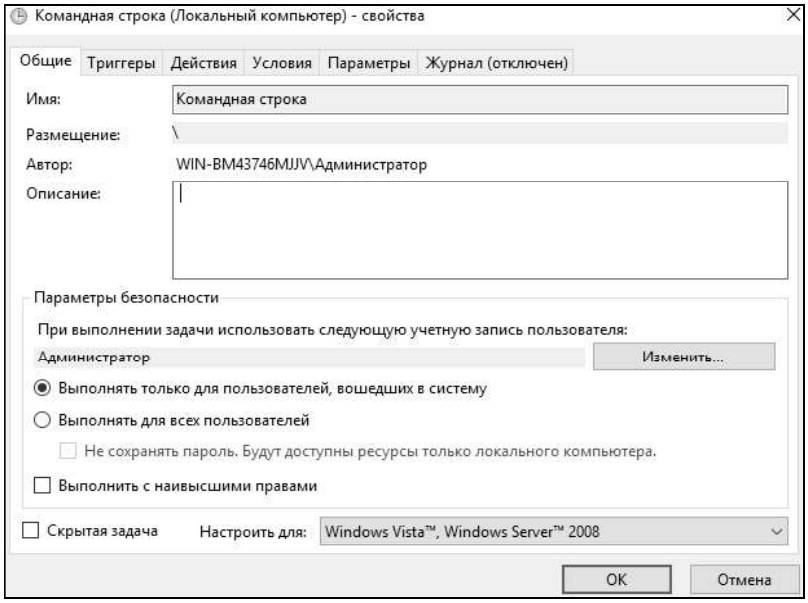

Рис. 25. Свойства задачи

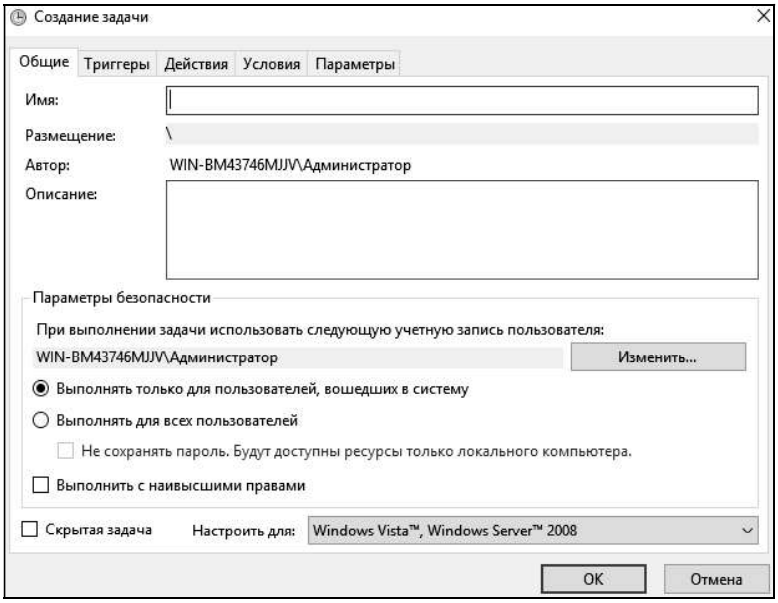

Рис. 26. Общие параметры создаваемой задачи

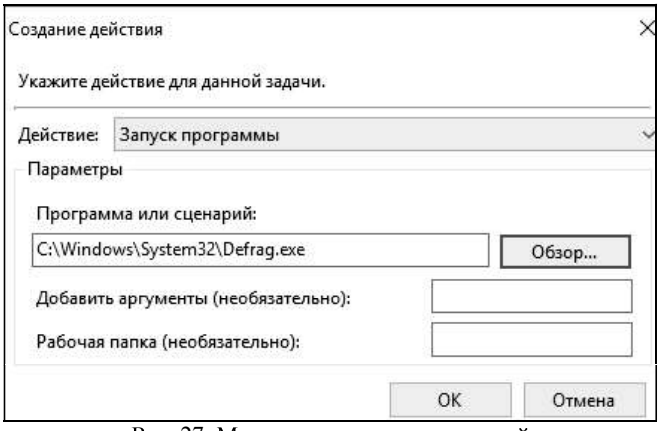

Рис. 27. Мастер планирования заданий

Ошибки при создании задачи, которые приводят к незапуску задачи в указанное время – неправильно введенный пароль, либо пароль не введен вообще. Путь к программе или скрипту, которые запускаются задачей, указан неправильно. Если в пути к запускаемой программе или скрипту есть пробелы, то путь должен быть заключен в кавычки. Еще необходимо проверить статус службы планировщика. Он должен быть запущен и режим запуска службы планировщик заданий должен быть «Авто».

3.3. Работа с процессами и потоками

Запустите «Process Explorer» (файл procexp.exe). В главном окне перечислены все работающие в системе процессы, представленные в виде древовидной структуры (рис. 28).

Двойной щелчок по имени процесса открывает окно его свойств (рис. 29). Свойства процесса предоставляют информацию о работе выбранного процесса. На вкладке «Образ» указаны путь к программе, родительский процесс, текущий рабочий каталог, предоставляется возможность уничтожения процесса и др. На вкладке «Производительность» выводится информация об использовании процессора, описание процесса, объем занятой памяти, на основе которых на вкладке «График производительности» построены графики.

Существует два режима работы программы. В режиме дескрипторов и в режиме библиотек DLL, переключение между режимами осуществляется с помощью сочетания клавиш Ctrl+H – переключение в режим отображения описателей и Ctrl+D – переключение в режим отображения DLL.

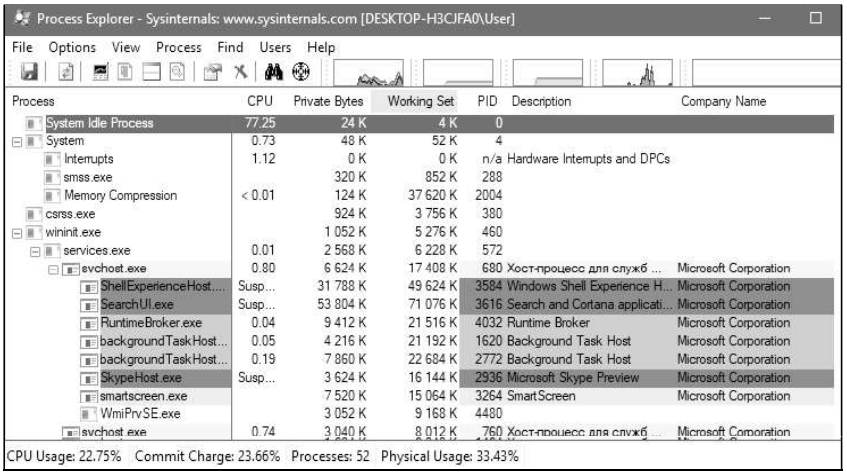

Рис. 28. Главное окно Process Explorer

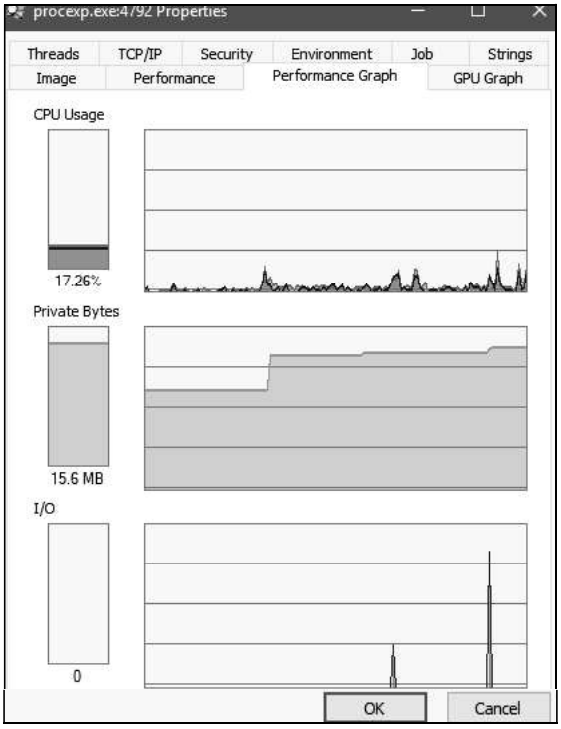

Рис. 29. Окно свойств процесса

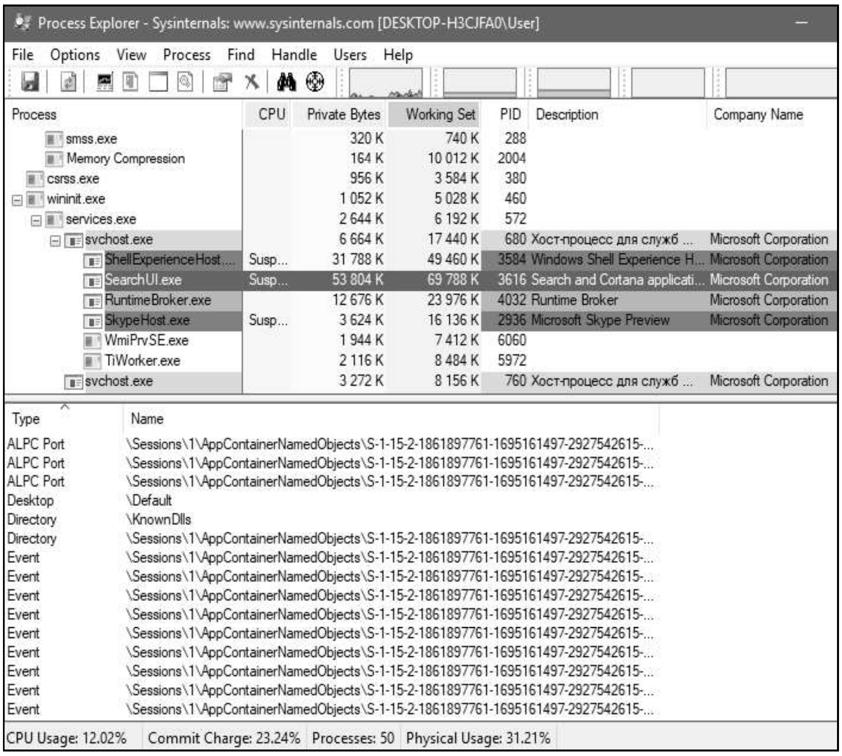

Рис. 30. Режим отображения дескрипторов

В режиме дескрипторов (рис. 30), в нижнем окне, отображаются все открытые дескрипторы выбранного в верхнем окне процесса, в данном случае, посмотрим дескрипторы открытые процессом procexp.exe: Section – диспетчер памяти объект «Секция» для общей памяти. Semaphore – исполнительная система определяет объекты «семафор». File – диспетчер ввода/вывода определяет объект «файл» для представления открытых экземпляров ресурсов драйверов устройств, которые включают в себя файлы файловой системы. Key – «ключ» для представления открытого ключа системного реестра. Диспетчер процессов создает объекты «поток» (Thread) и «процесс» (Process). Mutant – «мутант» внутреннее название для мьютекса.

В режиме библиотек DLL (рис. 31) отображаются все загруженные процессом динамические библиотеки и отображенные в память файлы.

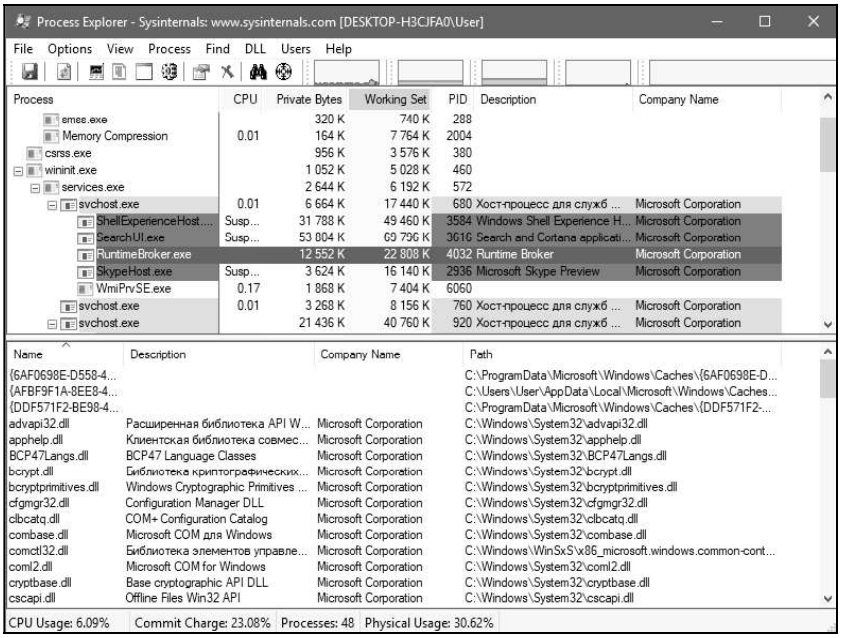

Рис. 31. Режим отображения библиотек DLL

Process Explorer позволяет приостановить/возобновить работу процесса, изменить приоритет, уничтожить процесс или уничтожить процесс и его дерево. Для этого необходимо щелкнуть на нужный процесс правой кнопкой мыши и в открывшемся контекстном меню выбрать необходимое действие. Например, в процесс explorer.exe, входит процесс procexp.exe, можно уничтожить это дерево процессов (рис. 32). Приостановка работы процесса может временно освободить занятые им ресурсы для использования другими приложениями.

Process Explorer предоставляет в распоряжение пользователя удобный инструмент, с помощью которого очень просто определить то, каким процессом открыто определенное окно. Для этого следует перетащить с панели инструментов Process Explorer кнопку в любое место открывшегося окна. После этого в верхней части главного окна будет подсвечено имя искомого процесса (рис. 33).

При помощи пункта меню «Параметры – Вместо диспетчера задач» можно заменить стандартный Диспетчер задач Windows на Process Explorer (рис. 34). Информация о системе, вызываемая из Process Explorer более полная, чем аналогичная вкладка Диспетчера задач Windows.

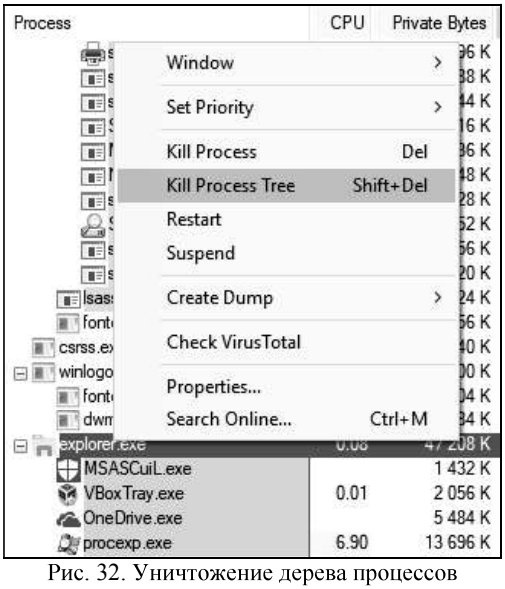

Рис. 32. Уничтожение дерева процессов

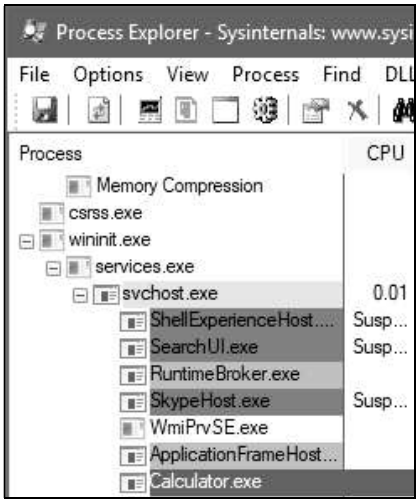

Рис. 33. Подсветка имени искомого процесса

При помощи пункта меню «Файл – Сохранить» (рис. 35), сохранить в текстовый файл список всех процессов с описаниями и объемом занятой каждым из них памяти.

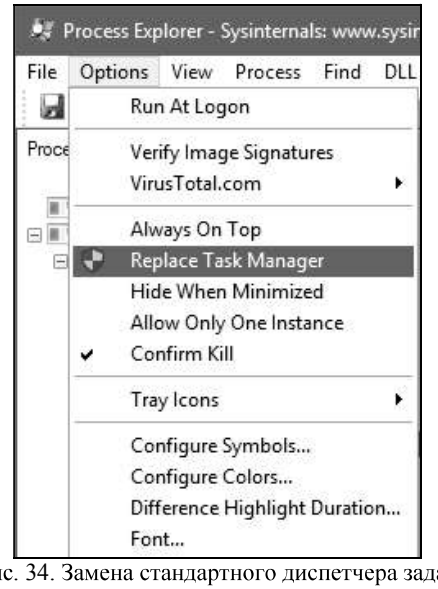

Рис. 34. Замена стандартного диспетчера задач

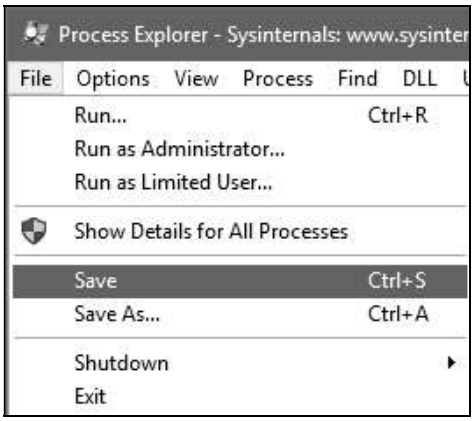

Рис. 35. Сохранение в текстовый файл списка всех процессов

Можно рассчитать влияние приоритета процесса на количество выделяемого процессорного времени, а также задать приоритет (приоритет можно выбрать при помощи нажатия правой кнопки мыши по процессу). На рис. 36 видно, сколько выделяется суммарного времени за одну минуту при заданном приоритете «Реального времени: 24» и 4 соответственно.

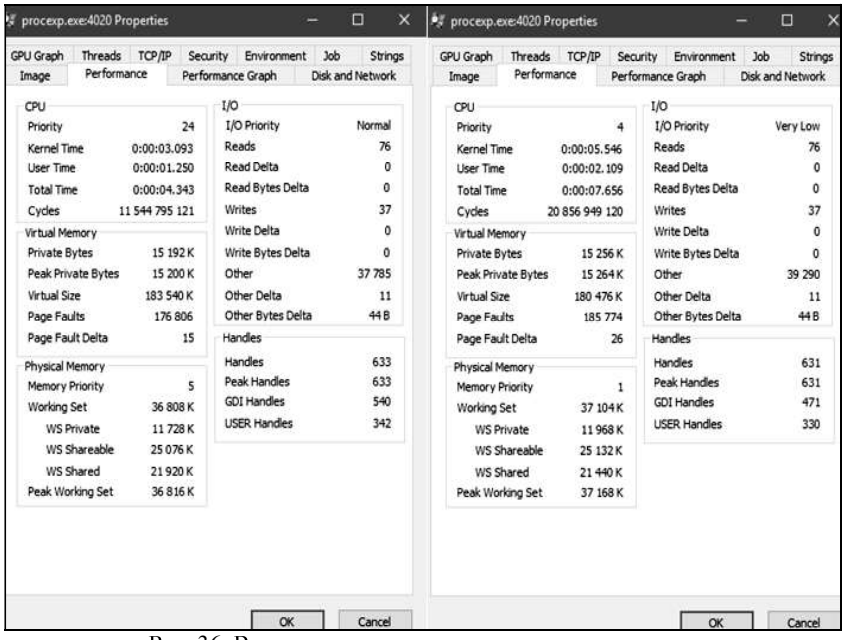

Рис. 36. Влияние приоритета на выделяемые ресурсы

У потоков, также как и у процессов, существует возможность менять приоритет, приоритет потока изменяется путем изменения приоритета у процесса. Аналогично процессам, потокам выделяется процессорное время, также потоки можно приостановить и уничтожить.

Чтобы просмотреть потоки, исполняемые в рамках процесса, необходимо открыть вкладку потоки в окне свойств процесса (рис. 37).

Чтобы просмотреть стек потока процесса, необходимо нажать клавишу «Stack» (рис. 38).

Запустите «Process Monitor» (файл ProcmonRus.exe). Откроется главное окно утилиты (рис. 39). В этом окне можно отследить действия процессов во время их работы.

При помощи меню «Файл – Сохранить» можно сохранить информацию о процессах в журнал (рис. 40).

С помощью утилиты Process Monitor можно отследить действия (включая «чтение» и «запись») процесса с файлами, реестром, сетью. Для этого необходимо зайти в меню «Настройки – Выбор колонок» и выбрать колонку «Категория» (рис. 41). В результате в колонке «Категория» можно увидеть действия процесса (рис. 42).

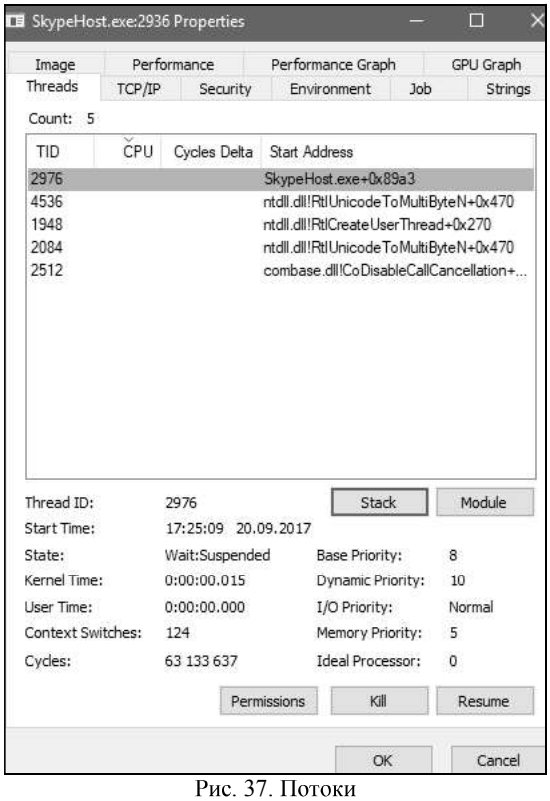

Рис. 37. Потоки

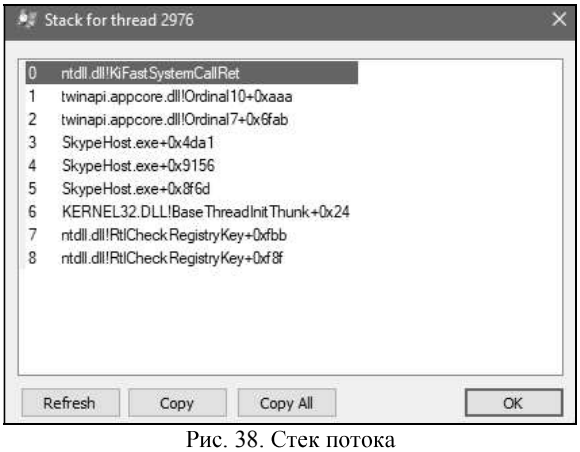

Рис. 38. Стек потока

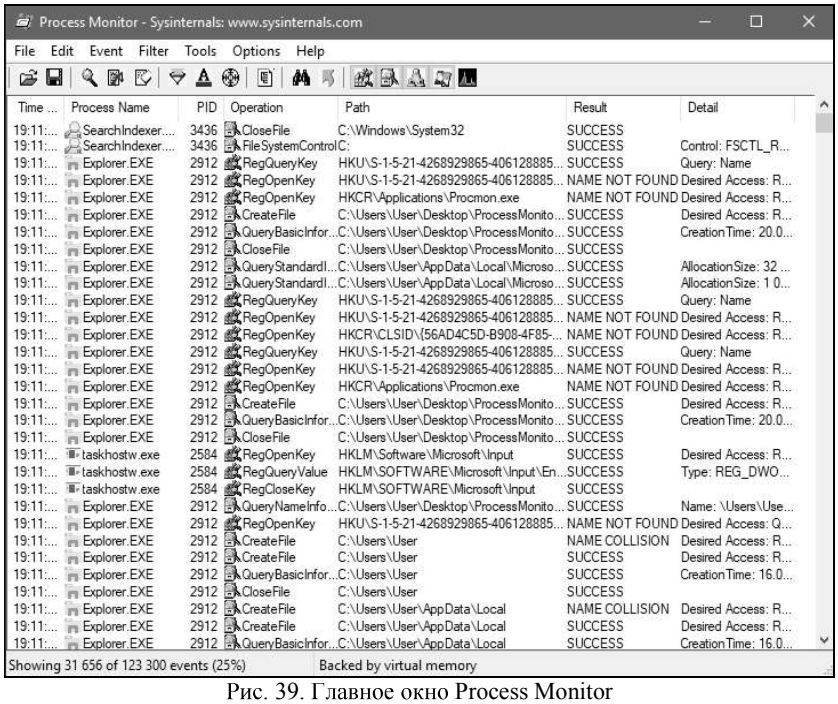

Рис. 39. Главное окно Process Monitor

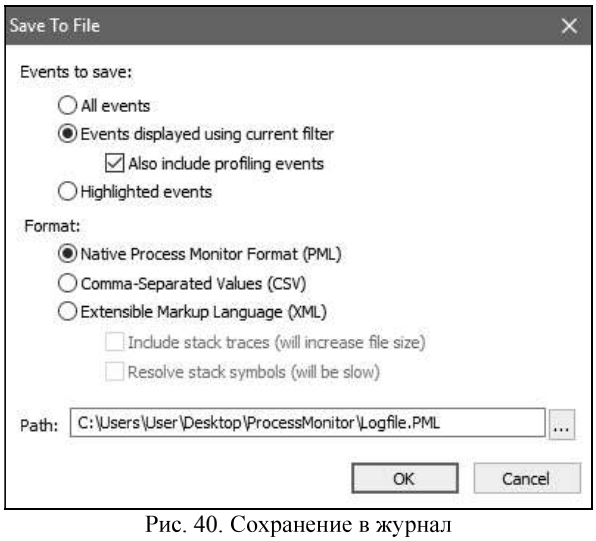

Рис. 40. Сохранение в журнал

Рис. 41. Выбор колонок

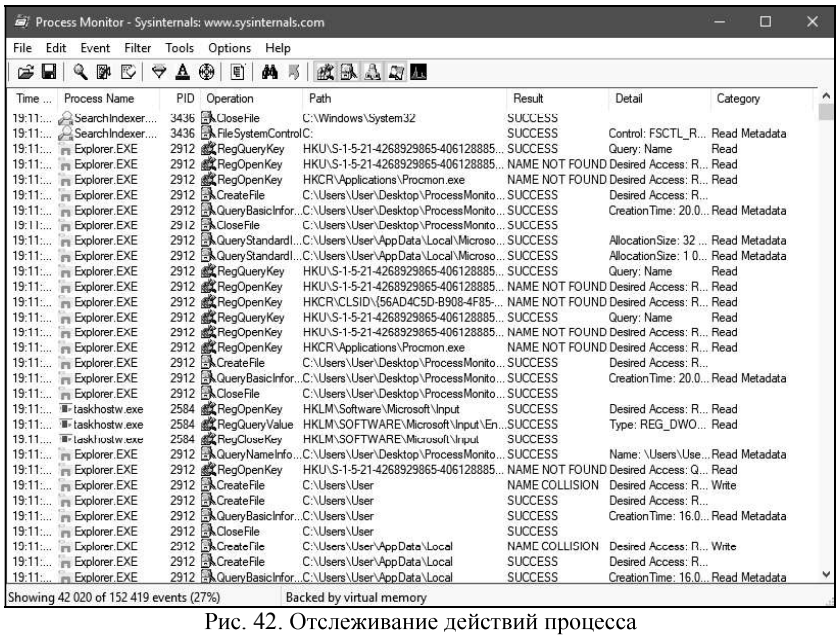

Рис. 42. Отслеживание действий процесса

Также можно отследить активность процессов при помощи меню «Инструменты – Лог активных процессов» (рис. 43).

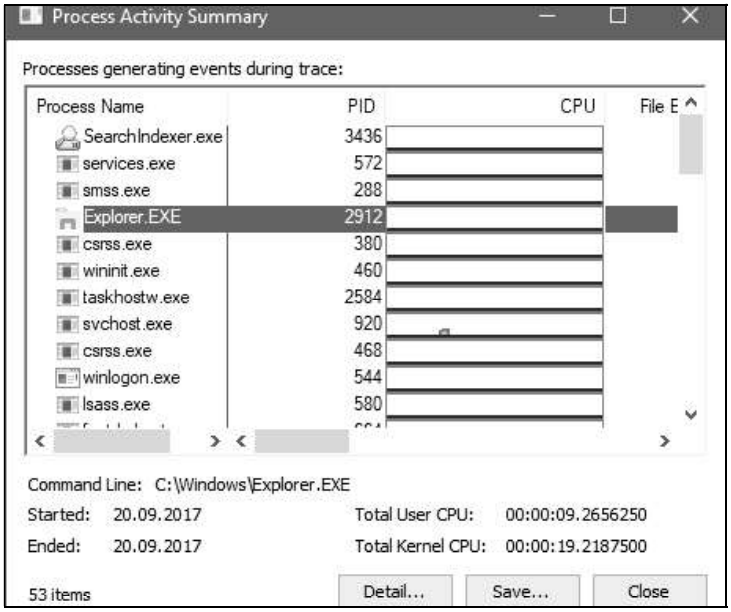

Рис. 43. Лог активных процессов

Process Monitor предоставляет возможность создавать фильтры, позволяющие делать выборки из журналов. Попасть в меню фильтров можно нажатием сочетания клавиш Ctrl+L. Фильтры можно создавать по многим параметрам, например, по имени процесса, времени, категории, операций и др. Создадим фильтр, который делает выборку процессов по операции записи в файл (рис. 44).

Также можно отследить работу процессов с файловой системой и реестром при установке программного обеспечения. Рассмотрим данную функцию на примере установки 7-zip. Установите программу. После установки выведите на экран информацию о записи ключей в реестр при установке программы. Для этого необходимо создать фильтр, который делает выборку процессов по операции записи в RegCreateFile. Определите, в каких разделах реестра 7-zip сохранил свою информацию. По аналогии определите, в каких каталогах диска были созданы новые данные.

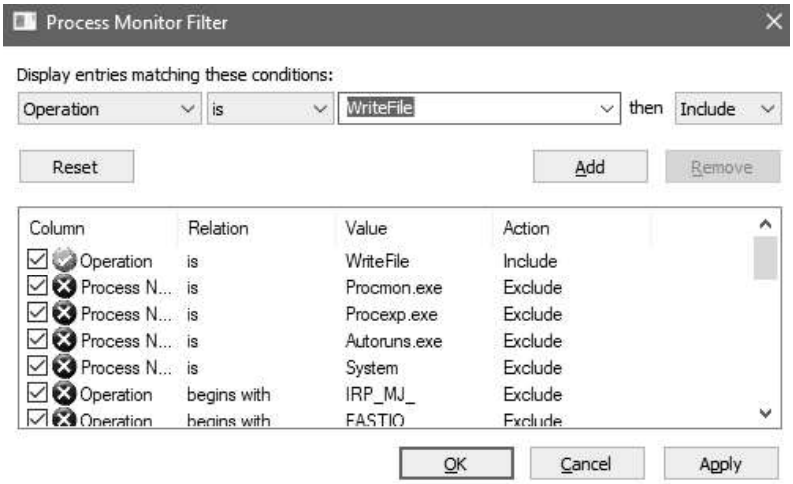

Рис. 44. Создание фильтра

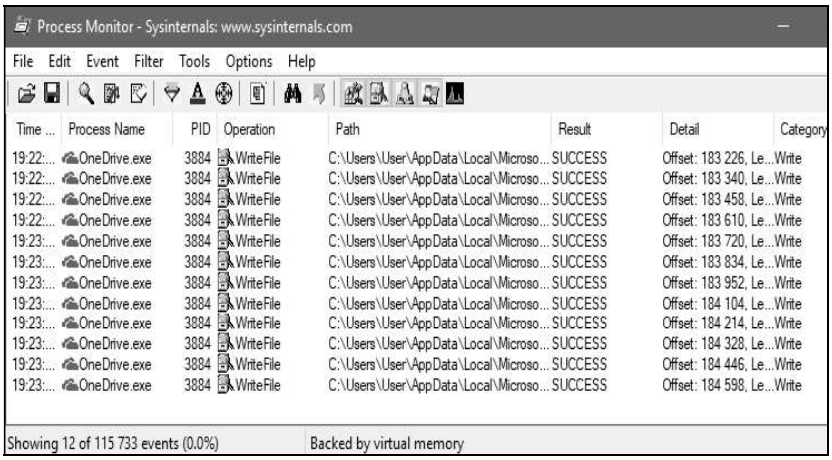

Рис. 45. Результат действия фильтра

4. Задание на лабораторную работу

1. Задать через командную строку перезагрузку компьютера через минуту после первого сбоя.
2. Назначить автоматический запуск калькулятора после входа в Windows.
3. Заменить стандартный диспетчер задач на Process Explorer.
4. Определить какой раздел реестра «Сапер» делает записи о рекордах.
5. Вывести информацию о Cookies при работе Internet Explorer.
6. Определить какие файлы реестра открывает косынка.
7. Определить какие системные файлы читает при работе WMPlayer.
8. Определить какой процесс запускается при открытии “Установки и удаления программ”.
9. Определить в какой файл записываются данные при работе с калькулятором.

5. Контрольные вопросы

1. Что такое служба Windows?
2. Какие средства для управления службами предусмотрены в Windows?
3. В каких состояниях может находиться служба?
4. Какие действия могут применяться при сбое службы?
5. Правами каких учётных записей может обладать служба при запуске?
6. Чем отличаются команды для управления службами семейств net и sc?
7. Какие команды используются для изменения состояния и типа запуска служб?
8. Чем отличается процесс от потока?
9. Как с помощью Process Explorer определить, каким процессом открыто определенное окно?
10. По каким параметрам можно создавать фильтры в Process Monitor?